HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

AF/2144
IFW

PATENT APPLICATION

ATTORNEY DOCKET NO. 10002142-1

O I P E JC48
DEC 0 6 2004
PATENT & TRADEMARK OFFICE

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Alexander C. Ranous et al.

Confirmation No.: 3043

Application No.: 09/560,032

Examiner: Michael Delgado

Filing Date: April 27, 2000

Group Art Unit: 2144

Title: INTERNET USAGE DATA RECORDING SYSTEM AND METHOD EMPLOYING A CONFIGURABLE RULE ENGINE FOR THE PROCESSING AND CORRELATION OF NETWORK DATA

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on **October 4, 2004**.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $340.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$110.00
( )	two months	$430.00
( )	three months	$980.00
( )	four months	$1530.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$340.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

(X) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit: **Dec. 3, 2004**

OR

( ) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number________ on ________

Number of pages:

Typed Name: **Steven E. Dicke**

Signature: Steven E. Dicke

Respectfully submitted,

Alexander C. Ranous et al.

By Steven E. Dicke

Steven E. Dicke

Attorney/Agent for Applicant(s)
Reg. No. **38,431**

Date: **Dec. 3, 2004**

Telephone No.: **(612) 573-2002**

OIPE JCIE
DEC 0 6 2004
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Alexander C. Ranous et al.	Examiner:	Michael Delgado
Serial No.:	09/560,032	Group Art Unit:	2144
Filed:	April 27, 2000	Docket No.:	10002142-1
Title:	INTERNET USAGE DATA RECORDING SYSTEM AND METHOD EMPLOYING A CONFIGURABLE RULE ENGINE FOR THE PROCESSING AND CORRELATION OF NETWORK DATA		

APPEAL BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appeal Brief

This brief is presented in support of the Notice of Appeal filed on October 4, 2004, from the final rejection dated July 2, 2004, and the Advisory Action dated September 23, 2004, of the Examiner rejecting claims 1-31 of the above identified application. Claims 1-31 remain for consideration.

The U.S. Patent and Trademark Office is hereby authorized the Charge Deposit Account No. 08-2025 in the amount of $340.00 for filing a Brief in Support of an Appeal as set forth under 37 C.F.R. 1.17(c), however, at any time during the pendency of this application, please charge any fees required or credit any overpayment to Deposit Account 08-2025 pursuant to 37 C.F.R. 1.25. Additionally, please charge any fees to Deposit Account 08-2025 under 37 C.F.R. 1.16, 1.17, 1.19, 1.20 and 1.21. Appellant respectfully requests reversal of the Examiner's rejection of pending claims 1-31.

12/07/2004 FMETEKI1 00000043 082025 09560032
01 FC:1402 340.00 DA

Table of Contents

Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP.

Related Appeals and Interferences

There are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this Appeal.

Status of Claims

Claims 1-31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,405,251 to Bullard et al. in view of U.S. Patent No. 5,970,490 to Morgenstern.

No claims have been allowed. Claims 1-31 are appealed herein.

Status of Amendments

No amendments have been entered subsequent to the Final Office Action mailed July 2, 2004. The claims listed in the Claims Appendix reflect the claims as of July 2, 2004. A Response After Final was filed on August 25, 2004, but no amendments to the claims were proposed by Appellants or entered by the Examiner.

Summary of Claimed Subject Matter

The Summary is set forth as an exemplary embodiment as the language corresponding to independent claims 1, 13, 17, 24, 26 and 30. Discussions about elements of claims 1, 13, 17, 24, 26 and 30 can be found at least at the cited locations in the specification and drawings.

The present invention, as claimed in independent claim 1, provides a method for recording network usage. The method comprises defining a network data collector including an encapsulator, an aggregator, and a data storage system. A set of network accounting data is received via the encapsulator. The network accounting data set is converted to a standard data format. The network accounting data set is processed via the aggregator, including defining a rule chain and applying the rule chain to the network accounting data set to

construct and aggregation tree including creating an aggregated network accounting data set. The aggregated network accounting data set is stored in the data storage system. See page 33, line 9 through page 35, line 22, and Figure 9, reference numbers 300-316. See also Figures 1-8.

The present invention, as claimed in independent claim 13, provides a method for recording network usage including correlating of network usage information and network session information. The method comprises defining a network data correlator collector including an encapsulator, an aggregator, and a data storage system. A set of network session data is received via the encapsulator. The network session data set is processed via the aggregator, including defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree. A set of network usage data is received via the encapsulator. The network usage data set is processed via the aggregator, including defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree. A correlated data set is determined from the correlated aggregation tree. The correlated data set is stored in the data storage system. See page 33, line 9 through page 39, line 2, and Figures 9-18, reference numbers 300-464.

The present invention, as claimed in independent claim 17, provides a method for recording network usage comprising defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system. A first set of network data is received via the first encapsulator. The first network data set is processed via the first aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data. The first aggregated network data set is stored in the first data storage system. See page 33, line 9 through page 35, line 22, and Figure 9, reference numbers 300-316. See also Figures 1-8.

The present invention, as claimed in independent claim 24, provides a network usage recording system having a network data collector. The network data collector comprises an encapsulator for receiving a set of network accounting data and converting the network accounting data set to a standard data format. An aggregator is provided for processing the network accounting data set, the aggregator including a defined rule chain, wherein the

aggregator applies the rule chain to the network accounting data set to construct an aggregation tree, and determines a set of aggregated network accounting data from the aggregation tree. A data storage system is provided for storing the aggregated network accounting data. See page 33, line 9 through page 35, line 22, and Figure 9, reference numbers 300-316. See also Figures 1-8.

The present invention, as claimed in independent claim 26, provides a network usage recording system having a network data correlator collector. The network data correlator collector comprises an encapsulator which receives a set of network session data. An aggregator for processing the network session data set, the aggregator including a defined first rule chain, wherein the aggregator applies the first rule chain to the network session data set to construct an aggregation tree. The encapsulator receives a set of network usage data, and the aggregator processes the network usage data set, the aggregator including a defined second rule chain, wherein the aggregator applies the second rule chain to the network usage data set and the aggregation tree to construct a correlated aggregation tree, and determines a correlated data set from the correlated aggregation tree. A data storage system is provided for storing the correlated data set. See page 33, line 9 through page 39, line 2, and Figures 9-18, reference numbers 300-464.

The present invention, as claimed in independent claim 30, provides a method for recording network usage. The method comprises defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system. A first set of network data is received via the first encapsulator. The first network data set is processed via the first aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data. The first aggregated network data set is stored in the first data storage system. Applying the aggregation rule chain to the first set of network data further comprises constructing an aggregation tree, and determining the first aggregated network data set from the aggregation tree. Constructing an aggregation tree further includes defining the first network data set to include a first network data event in a second network data event. The aggregation rule chain is applied to the first network data event to construct a hierarchy of group nodes within the aggregation tree. The aggregation rule chain is applied to the second network data event to

located similar group nodes according to a predefined set of match rules. If no matching group nodes exist, the hierarchy of group nodes is extended within the aggregation tree by creating additional group nodes. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a first a match rule for matching source IP address. The first network data event is defined to include a first source IP address. The first match rule is applied to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address. If a matching first group node does exist, the first group node is created for the first source IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a second match rule for matching destination IP address. The first network data event is defined to include a first destination IP address. The second match rules apply to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address. If a matching second group node does not exist, the second group node is created for the first destination IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule set to include an aggregation rule. Defining the first network data event to include a port number and volume of information, and applying the aggregation rule to the first network data event including copying the port number, source IP address, destination IP address and volume information to the second group node. See page 33, line 9 through page 39, line 2, and Figures 9-18, reference numbers 300-464.

Grounds of Rejection to be Reviewed on Appeal

Claims 1-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,405,251 to Bullard et al. in view of U.S. Patent No. 5,970,490 to Morgenstern.

Argument

I. *The rejection of claims 1-31 under 35 U.S.C. 103(a)*

Claims 1-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,405,251 by Bullard et al. ("Bullard") in view of U.S. Patent No. 5,970,490 by Morgenstern ("Morgenstern"). Appellants submit that the Bullard reference alone or in combination with the Morgenstern reference fails to disclose, teach, or suggest the invention of independent claims 1, 13, 17, 24, 26 and 30 and the claims depending therefrom.

A. The rejection of claims 1-12 and 17-25 under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern

The rejection of claims 1-12 and 17-25 in the Final Office Action mailed July 2, 2004, under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern is not correct and should be withdrawn, because the rejection fails to establish a case of *prima facie* obviousness.

Referring to Section 706.02 (j) of the MPEP, to establish a *prima facie* case of obviousness, three basic criteria must be met:

(1) There must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference to combine reference teachings;
(2) There must be reasonable expectation of success;
(3) The prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on Appellant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (F.E.D. Cir. 1991).

Independent claim 1 recites a method for recording network usage. The method comprises defining a network data collector including an encapsulator, an aggregator, and a data storage system. A set of network accounting data is received via the encapsulator. A network accounting data set is converted to a standard data format. The network accounting data set is processed via the aggregator, including defining a rule chain and applying the rule

chain to the network accounting data set to construct an aggregation tree including creating an aggregated network accounting data set. The aggregated network accounting data set is stored in the data storage system.

Bullard discloses a system for enhancement of network accounting records. The system includes a data collector layer 18 that is a distributed layer of individual data collectors. The data collectors collect raw accounting information and convert data into normalized records referred to as network accounting records (NARs). Each of the data collectors forwards network accounting records to a flow aggregation process 60. (See column 3, lines 43-54). The flow aggregation process 60, including aggregation processor 13, is a central collection point for all network accounting records produced from various data collectors in the data collection layer 18. The flow aggregation processor 60 aggregates and/or enhances record data across the network devices to produce summary NARs' (column 4, lines 1-26), and (column 18, lines 39-49). The data can be further enhanced and/or reduced (i.e., aggregated) to meet the specific needs of an application or output interface based on the aggregation policy of the flow data processor 60.

Morgenstern discloses an integration system for processing heterogeneous data from multiple sources. The integration system utilizes an interoperability assistant module 20 (figure 2) including specifications for transforming the heterogeneous data into a common intermediate representation of the heterogeneous data using the specifications and creating an information bridge with the interoperability assistant module through a process of program generation. (See col. 1, lines 10-17). The system provides high-level user interfaces and program level access across heterogeneous databases, allowing immigration of a variety of information resources including relational and object databases, CAD design tools, simulation packages, data analysis and visualization tools, and other software modules. (Col. 3, lines 7-13).

High level transformation rule specifications (HLTRS) are utilized by the system to transform data from a source data representation to a target data representation. (See col. 8, lines 5-8). The HLTRS are sent to a transformer generator 42, which generates code files that describe the transformation rules in a form usable by a dependency graph 200 (see figure 4), which controls the data flow from source to target. (Col. 8, lines 53-57). Dependency graph

200 is the basis for rule execution. Dependency graph 200 is composed of an input tree 210, a rule graph 220, and an output tree 230. (See fig. 4 and col. 20, lines 46-50). Input data instances are first inserted into the input tree. The data instances are then passed by the input tree to the rule graph, together with completion signals. The rule graph 220 will apply specified transformation rules on the data instances to generate intermediate instances and output instances. The final rules of the rule graph insert the output instances into the output tree 230, which assembles and eventually outputs them accordingly. (Col. 21, lines 19-23).

The examiner conceded that Bullard does not teach **processing the network accounting data set via the aggregator, including the steps of defining a rule chain and applying the rule chain to the network accounting data set to construct an aggregation tree including creating an aggregated network accounting data set.** (Final Office Action, pg. 3 and pg. 4; See also pg. 2 Response to Arguments, paragraph 1). The examiner submits that this limitation is taught by Morgenstern.

Morgenstern also does not disclose **defining a rule chain and applying the rule chain to the network accounting data to construct an aggregation tree including creating an aggregated network accounting data set** as claimed by Appellants. The mere use of the terms "rule" and "tree" in Morgenstern does not disclose Appellants' claimed invention. Morgenstern merely discloses a rule graph 220, an input tree 210 and output tree 230. The rule graph 220 is a directed graph and consists of data nodes and rule nodes. Each rule node is connected to one or more input data nodes and no more than one output data node. (See col. 21, lines 41-44). Rule graph 220 is not a rule chain as claimed by Appellants. In Morgenstern, **input data instances are first inserted into the input tree. The data instances are then passed by the input tree to the rule graph, together with completion signals.** The rule graph 220 will apply specified transformation rules on the data instances to generate intermediate instances and output instances. The final rules of the rule graph insert the output instances into the output tree 230 which assembles and eventually outputs them accordingly. (See Morgenstern, Col. 21, lines 19-26). [Emphasis Added].

In contrast, Appellants **apply a rule chain to the network accounting data set to construct an aggregation tree including an aggregated network accounting data set.** In

view of the above, one skilled in the art could not combine the teachings of Bullard in view of Morgenstern and arrive at the present invention of independent claim 1.

Further, even if Bullard in combination with Morgenstern disclosed Applicants claimed invention of independent claim 1, Bullard and Morgenstern fail to teach or suggest such a combination. Again, Bullard fails to teach or suggest defining a rule chain and applying the rule chain to a network accounting data set to construct an aggregation tree. Morgenstern is directed to a method for processing heterogeneous data and does not disclose or even relate to collecting network accounting data as claimed by Appellants. Rather, Morgenstern is direct to heterogeneous databases for design, engineering and manufacturing applications (e.g., computer aided design). It would not be obvious to one skilled in the art to apply the teachings of Bullard in view of Morgenstern's design and engineering database and arrive at the present invention.

In view of the above, Applicants respectfully submit that the above rejection of independent claim 1 under 35 U.S.C. 103(a) should be withdrawn.

Independent claims 17 and 24 are grouped with independent claim 1, and also believed to be allowable over the art of record. Dependent claims 2-12, 18-23, and 25 depend directly or indirectly upon corresponding independent claims 1, 17 and 24. Accordingly, dependent claims 2-12, 18-23, and 25 are also allowable over the art of record.

B. The rejection of claims 13-16 and 26-29 under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern

The rejection of claims 13-16 and 26-29 in the Final Office Action mailed July 2, 2004, under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern is not correct and should be withdrawn, because the rejection fails to establish a case of *prima facie* obviousness.

Referring to Section 706.02 (j) of the MPEP, to establish a *prima facie* case of obviousness, three basic criteria must be met:

(1) There must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference to combine reference teachings;
(2) There must be reasonable expectation of success;

(3) The prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on Appellant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (F.E.D. Cir. 1991).

Independent claim 13 recites a method for recording network usage including correlating of network usage information and network session information. The method includes defining a network data correlator collector including an encapsulator, an aggregator, and a data storage system. A set of network session data is received via the encapsulator. The network session data set is processed via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree. A set of network usage data is received via the encapsulator. The network usage data set is processed via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree. A correlated data set is determined from the correlated aggregation tree. The correlated data set is stored in the data storage system.

Bullard is as discussed above under Section IA.

Morgenstern is as discussed above under Section IA.

As conceded by the Examiner, Bullard fails to disclose **processing a network session data set via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree, and processing a network usage data set via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree, and determining a correlated data set from the correlated aggregation tree.** (Final Office Action, p. 7).

Morgenstern also does not disclose **defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree** as claimed by Appellants. Morgenstern merely discloses a rule graph 220 and an input tree 210 and an

output tree 230. The rule graph 220 is a directed graph and consists of data nodes and rule nodes. Each rule node is connected to one or more input data nodes and no more than one output data node. (See col. 21, lines 41-44). Rule graph 220 is not a rule chain as claimed by Applicant. In Morgenstern, **input data instances are first inserted into the input tree. The data instances are then passed by the input tree to the rule graph, together with completion signals.** The rule graph 220 will apply specific transformation rules on the data instances to generate intermediate instances and output instances. The final rules of the rule graph insert the output instances into the output tree 230 which assembles and eventually outputs them accordingly. (See Morgenstern, col. 21, lines 19-26). [Emphasis Added]

In contrast, Applicants **apply the first rule chain to the network session data to construct an aggregation tree.** In further contrast to Morgenstern, **Appellants define a second rule chain and apply the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree, and determine a correlated data set from the correlated aggregation tree**, none of which is disclosed in Morgenstern. In view of the above, one skilled in the art could not combine the teachings of Bullard in view of Morgenstern and arrive at the present invention of independent claim 13. Accordingly, Appellants respectfully submit that the above rejection of independent claim 13 under 35 U.S.C. 103(a) should be withdrawn.

Further, even if Bullard and Morgenstern in combination disclosed Applicants invention of independent claim 13, Bullard and Morgenstern fail to teach or suggest such a combination. Again, Bullard fails to teach or suggest defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree, and processing a network usage data set via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree. Morgenstern is directed to a method for processing heterogeneous data and does not disclose or even relate to collecting network accounting data. Rather, Morgenstern is directed to heterogeneous databases for design, engineering and manufacturing applications (e.g., computer aided design). It would not be obvious to one skilled in the art to apply the teachings of Ballard in view of Morgenstern's design and engineering database and arrive at the present invention.

In view of the above, Appellants respectfully submit that the above rejection of independent claim 13 under 35 U.S.C. § 103(a) should be withdrawn.

Independent claim 26 is grouped with Independent claim 13 and believed to be patentable. Dependent claims 14-16 and 27-29 depend directly or indirectly upon independent claim 13. Accordingly, dependent claims 14-16 and 27-29 are also allowable over the art of record.

C. The rejection of claims 30 and 31 under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern

The rejection of claims 30 and 31 in the Final Office Action mailed July 2, 2004 under 35 U.S.C. § 103(a) as being unpatentable over Bullard in view of Morgenstern is not correct and should be withdrawn, because the rejection fails to establish a case of *prima facie* obviousness.

Referring to Section 706.02 (j) of the MPEP, to establish a *prima facie* case of obviousness, three basic criteria must be met:

(1) There must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference to combine reference teachings;
(2) There must be reasonable expectation of success;
(3) The prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on Appellant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (F.E.D. Cir. 1991).

Independent claim 30 recites defining a first network data collector including a first encapsulator, a first aggregator, and a first data storage system. A first set of network data is received via the first encapsulator. The first network data set is processed via the first aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data. The first aggregated network data set is stored in the first data storage system.

Applying the aggregation rule chain to the first set of network data further comprises constructing an aggregation tree. The first aggregated network data set is determined from the aggregation tree, where constructing an aggregation tree includes defining the first network data set to include a first network data event and a second network data event. The aggregation rule chain is applied to the first network data event to construct a hierarchy of group nodes within the aggregation tree. The aggregation rule chain is applied to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, the hierarchy of group nodes is extended within the aggregation tree by creating additional group nodes.

Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a first match rule for matching source IP address. The first network data event is defined to include a first source IP address. The first match rule is applied to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address, and if a matching first group node does not exist, creating the first group node for the first source IP address.

Applying the aggregation rule chain to the first network data event includes defining the aggregation rule chain to include a second match rule for matching destination IP address. The first network data event is defined to include a first destination IP address. The second match rule is applied to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address, and if a matching second group node does not exist, creating the second group node for the first destination IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule set to include an aggregation rule. The first network data event is defined to include a port number and volume of information. The aggregation rule is applied to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node. Bullard and Morgenstern do not teach or suggest these claim recitations.

Bullard is as discussed above in Section IA.

Morgenstern is as discussed above in Section IA.

As conceded by the Examiner, Bullard fails to disclose **a network data set processed via the aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data.** As further conceded, Bullard fails to disclose **applying the aggregation rule chain to the first set of network data further comprises constructing an aggregation tree. The first aggregated network data set is determined from the aggregation tree, where constructing an aggregation tree includes defining the first network data set to include a first network data event and a second network data event. The aggregation rule chain is applied to the first network data event to construct a hierarchy of group nodes within the aggregation tree. The aggregation rule chain is applied to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, the hierarchy of group nodes is extended within the aggregation tree by creating additional group nodes.**

Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a first match rule for matching source IP address. The first network data event is defined to include a first source IP address. The first match rule is applied to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address, and if a matching first group node does not exist, creating the first group node for the first source IP address.

Applying the aggregation rule chain to the first network data event includes defining the aggregation rule chain to include a second match rule for matching destination IP address. The first network data event is defined to include a first destination IP address. The second match rule is applied to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address, and if a matching second group node does not exist, creating the second group node for the first destination IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule set to include an aggregation rule. The first network data event is defined to include a port number and volume of information. The aggregation rule is

applied to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node. (Final Office Action, pages 13-16).

Morgenstern also does not disclose **a network data set processed via the aggregator, including defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data** as claimed by Appellants. Morgenstern merely discloses a rule graph 220 and an input tree 210 and an output tree 230. The rule graph 220 is a directed graph and consists of data nodes and rule nodes. Each rule node is connected to one or more input data nodes and no more than one output data node. (See col. 21, lines 41-44). Rule graph 220 is not a rule chain as claimed by Applicant. In Morgenstern, **input data instances are first inserted into the input tree. The data instances are then passed by the input tree to the rule graph, together with completion signals.** The rule graph 220 will apply specific transformation rules on the data instances to generate intermediate instances and output instances. The final rules of the rule graph insert the output instances into the output tree 230 which assembles and eventually outputs them accordingly. (See Morgenstern, col. 21, lines 19-26). [Emphasis Added]

In contrast, Appellants **apply the aggregation rule chain to the first set of network data to construct an aggregation tree.** In further contrast to Morgenstern, **Appellants define a second rule chain and apply the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree. The first aggregated network data set is determined from the aggregation tree, where constructing an aggregation tree includes defining the first network data set to include a first network data event and a second network data event. The aggregation rule chain is applied to the first network data event to construct a hierarchy of group nodes within the aggregation tree. The aggregation rule chain is applied to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, the hierarchy of group nodes is extended within the aggregation tree by creating additional group nodes.**

Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule chain to include a first match rule for matching source IP address. The first network data event is defined to include a first source IP address. The first match rule is applied to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address, and if a matching first group node does not exist, creating the first group node for the first source IP address.

Applying the aggregation rule chain to the first network data event includes defining the aggregation rule chain to include a second match rule for matching destination IP address. The first network data event is defined to include a first destination IP address. The second match rule is applied to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address, and if a matching second group node does not exist, creating the second group node for the first destination IP address. Applying the aggregation rule chain to the first network data event further includes defining the aggregation rule set to include an aggregation rule. The first network data event is defined to include a port number and volume of information. The aggregation rule is applied to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node. None of the above is disclosed in Morgenstern. In view of the above, one skilled in the art could not combine the teachings of Bullard in view of Morgenstern and arrive at the present invention of independent claim 30. Accordingly, Applicants respectfully submit that the above rejection of independent claim 30 under 35 U.S.C. 103(a) should be withdrawn.

Further, even if Bullard and Morgenstern in combination disclosed Appellants invention of independent claim 30, Bullard and Morgenstern fail to teach or suggest such a combination. Again, Bullard fails to teach or suggest a method for recording network usage as claimed above. Again, Morgenstern merely discloses a rule graph, input tree and output tree used in a design and engineering database (See Fig. 4). Morgenstern is directed to a method for processing heterogeneous data and does not disclose or even relate to collecting network accounting data as claimed in independent claim 30. Rather, Morgenstern is

directed to heterogeneous databases for design, engineering and manufacturing applications (e.g., computer aided design).

In view of the above, Appellants respectfully submit that the above rejection of independent claim 30 under 35 U.S.C. § 103(a) should be withdrawn.

Dependent claim 31 depends directly upon independent claim 30. Accordingly, this dependent claim is allowable over the art of record.

Conclusion

For above reasons, Appellants respectfully submit that the cited art neither anticipates nor renders the claimed invention obvious, and therefore the claimed invention does patentably distinguish over the cited art. Therefore, Appellants respectfully submit that the rejections to pending claims 1-31 are in error. Thus, Appellants respectfully request that the Board reverse the Examiner and find all pending claims allowable.

Any inquiry regarding this Appeal Brief to the Board of Patent Appeals and Interferences of the United States Patent and Trademark Office should be directed to either Steven E. Dicke at Telephone No. (612) 573-2002, Facsimile No. (612) 573-2005 or Philip S. Lyren at Telephone No. (281) 514-8236, Facsimile No. (281) 514-8332. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
3404 E. Harmony Road, M/S 35
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Alexander C. Ranous,

By their attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2002
Facsimile: (612) 573-2005

Date: December 3, 2004
SED:jan

Steven E. Dicke
Steven E. Dicke
Reg. No. 38,431

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this day of December, 2004.

By Steven E. Dicke
Name: Steven E. Dicke

O I P E JC48
DEC 0 6 2004
PATENT & TRADEMARK OFFICE

Claims Appendix

1. (Original) A method for recording network usage, the method comprising the steps of:

defining a network data collector including an encapsulator, an aggregator, and a data storage system;

receiving a set of network accounting data via the encapsulator;

converting the network accounting data set to a standard data format;

processing the network accounting data set via the aggregator, including the steps of defining a rule chain and applying the rule chain to the network accounting data set to construct an aggregation tree including creating an aggregated network accounting data set; and

storing the aggregated network accounting data set in the data storage system.

2. (Original) The method of claim 1, wherein the step of applying the rule chain to the network accounting data set to construct the aggregation tree includes the step of applying a rule from the rule chain to the network accounting data set to define a group node.

3. (Original) The method of claim 2, wherein the rule is a match rule.

4. (Original) The method of claim 1, wherein the step of applying the rule chain to the network accounting data set to construct the aggregation tree includes the step of

applying a set of match rules to the network accounting data set to define a hierarchy of group nodes within the aggregation tree.

5. (Original) The method of claim 4, wherein the step of applying the rule chain to the network accounting data set to construct the aggregation tree includes the step of applying an aggregation rule to the match group node to create the aggregated network accounting data set.

6. (Original) The method of claim 1, wherein the step of applying the rule chain to the network accounting data set to construct the aggregation tree includes the step of applying a data manipulation rule to the network accounting data set.

7. (Original) The method of claim 6, further comprising the step of defining the data manipulation rule to be an adornment rule.

8. (Original) The method of claim 6, further comprising the step of defining the data manipulation rule to be a filtering rule.

9. (Original) The method of claim 1, wherein the network accounting data set is a set of session data.

10. (Original) The method of claim 1, wherein the network accounting data set is a set of usage data.

11. (Original) The method of claim 1, further comprising the step of defining a data flush interval; and wherein the step of storing the aggregated network accounting data set

includes the step of transferring the aggregated network accounting data to the data storage system after a period of time associated with the data flush interval.

12. (Original) The method of claim 1, further comprising the step of defining a rule within the rule chain by a Java object class, and allowing additional rule types to be added to the rule chain corresponding to the Java object class.

13. (Original) A method for recording network usage including correlating of network usage information and network session information, the method comprising the steps of:

defining a network data correlator collector including an encapsulator, an aggregator,
and a data storage system;

receiving a set of network session data via the encapsulator;

processing the network session data set via the aggregator, including the steps of defining a first rule chain and applying the first rule chain to the network session data to construct an aggregation tree;

receiving a set of network usage data via the encapsulator;

processing the network usage data set via the aggregator, including the steps of defining a second rule chain and applying the second rule chain to the network usage data and the aggregation tree to construct a correlated aggregation tree;

determining a correlated data set from the correlated aggregation tree; and

storing the correlated data set in the data storage system.

14. (Original) The method of claim 13, wherein the network session data set is in a standard data format received from a session data collector having an encapsulator, an aggregator and a data storage system.

15. (Original) The method of claim 14, wherein the network usage data set is in the standard data format received from a usage data collector having an encapsulator, an aggregator and a data storage system

16. (Original) The method of claim 13, further comprising the step of defining the first rule set to be different than the second rule set.

17. (Original) A method for recording network usage comprising the steps of:

defining a first network data collector including a first encapsulator, a first aggregator,

and a first data storage system;

receiving a first set of network data via the first encapsulator;

processing the first network data set via the first aggregator, including the steps of defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data; and

storing the first aggregated network data set in the first data storage system.

18. (Original) The method of claim of claim 17, wherein the step of applying the aggregation rule chain to the first set of network data further comprises the steps of:

constructing an aggregation tree; and

determining the first aggregated network data set from the aggregation tree.

19. (Original) The method of claim 18, wherein the step of constructing an aggregation tree further includes the steps of:

defining the first network data set to includes a first network data event and a second
network data event;

applying the aggregation rule chain to the first network data event to construct a hierarchy of group nodes within the aggregation tree; and

applying the aggregation rule chain to the second network data event to locate similar
group nodes according to a predefined set of match rules, if no matching group nodes exist, extending the hierarchy of group nodes within the aggregation tree by creating additional group nodes.

20. (Original) The method of claim 19, wherein the step of applying the aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule chain to include a first match rule for matching source
IP address;

defining the first network data event to include a first source IP address;

applying the first match rule to the first network data event, including determining whether the aggregation tree includes a first group node matching the first source IP address; and

if a matching first group node does not exist, creating the first group node for the first
source IP address.

21. (Original) The method of claim 20, wherein the step of applying aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule chain to include a second match rule for matching destination IP address;

defining the first network data event to include a first destination IP address;

applying the second match rule to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address; and

if a matching second group node does not exist, creating the second group node for the first destination IP address.

22. (Original) The method of claim 21, wherein the step of applying the aggregation rule chain to the first network data event further includes the steps of:

defining the aggregation rule set to include an aggregation rule;

defining the first network data event to include a port number and volume of information;

applying the aggregation rule to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node.

23. (Original) The method of claim 17, further comprising the steps of:

defining a second network data collector including a second encapsulator, a second aggregator, and a second data storage system;

receiving a second set of network data via the second network encapsulator;

processing the second network data set via the second aggregator, including the steps of defining a second rule chain and applying the second rule chain to the second set of network data to define a second set of aggregated network data; and

storing the second aggregated network data set in the second data storage system.

24. (Original) A network usage recording system having a network data collector, the network data collector comprising:

an encapsulator for receiving a set of network accounting data and converting the network accounting data set to a standard data format;

an aggregator for processing the network accounting data set, the aggregator including a defined rule chain, wherein the aggregator applies the rule chain to the network accounting data set to construct an aggregation tree, and determines a set of aggregated network accounting data from the aggregation tree; and

a data storage system for storing the aggregated network accounting data.

25. (Original) The system of claim 24, wherein the process of applying the rule chain to the network accounting data performs data reduction on the network data.

26. (Original) A network usage recording system having a network data correlator collector, the network data correlator collector comprising:

an encapsulator which receives a set of network session data;

an aggregator for processing the network session data set, the aggregator including a

defined first rule chain, wherein the aggregator applies the first rule chain to the network session data set to construct an aggregation tree;

wherein the encapsulator receives a set of network usage data, and the aggregator processes the network usage data set, the aggregator including a defined second rule chain, wherein the aggregator applies the second rule chain to the network usage data set and the aggregation tree to construct a correlated aggregation tree, and determines a correlated data set from the correlated aggregation tree; and

a data storage system for storing the correlated data set.

27. (Original) The system of claim 26, wherein the network session data set is in a standard data format received from a session data collector having an encapsulator, an aggregator and a data storage system.

28. (Original) The system of claim 27, wherein the network usage data set is in the standard data format received from a usage data collector having an encapsulator, an aggregator and a data storage system.

29. (Original) The system of claim 26, further wherein the first rule set is different than the second rule set.

30. (Previously Presented) A method for recording network usage comprising:

defining a first network data collector including a first encapsulator, a first aggregator,

and a first data storage system;

receiving a first set of network data via the first encapsulator;

processing the first network data set via the first aggregator, including the steps of

defining an aggregation rule chain and determining a first set of aggregated data by applying the aggregation rule chain to the first set of network data; and

storing the first aggregated network data set in the first data storage system;

wherein applying the aggregation rule chain to the first set of network data further comprises:

constructing an aggregation tree; and

determining the first aggregated network data set from the aggregation tree;

wherein constructing an aggregation tree further includes defining the first network data set to includes a first network data event and a second network data event;

applying the aggregation rule chain to the first network data event to construct a hierarchy of group nodes within the aggregation tree; and

applying the aggregation rule chain to the second network data event to locate similar group nodes according to a predefined set of match rules, if no matching group nodes exist, extending the hierarchy of group nodes within the aggregation tree by creating additional group nodes;

wherein applying the aggregation rule chain to the first network data event further includes:

defining the aggregation rule chain to include a first match rule for matching source IP address;

defining the first network data event to include a first source IP address;

applying the first match rule to the first network data event,

---

including determining whether the aggregation tree includes a first group node matching the first source IP address; and if a matching first group node does not exist, creating the first group node for the first source IP address;

wherein applying aggregation rule chain to the first network data event further includes:

defining the aggregation rule chain to include a second match rule for matching destination IP address;

defining the first network data event to include a first destination IP address;

applying the second match rule to the first network data event, including determining whether the aggregation tree includes a second group node matching the first destination IP address; and if a matching second group node does not exist, creating the second group node for the first destination IP address;

wherein applying the aggregation rule chain to the first network data event further includes:

defining the aggregation rule set to include an aggregation rule;

defining the first network data event to include a port number and volume of information;

applying the aggregation rule to the first network data event, including copying the port number, source IP address, destination IP address and volume information to the second group node.

31. (Previously Presented) The method of claim 30, further comprising:

defining a second network data collector including a second encapsulator, a second

aggregator, and a second data storage system;

receiving a second set of network data via the second network encapsulator;

processing the second network data set via the second aggregator, including:

defining a second rule chain and applying the second rule chain to the second

set of network data to define a second set of aggregated network data; and

storing the second aggregated network data set in the second data storage system.